UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	CASE NO. CR11-70RAJ
	)	
v.	)	SEATTLE, WASHINGTON
	)	June 23, 2016
ROMAN SELEZNEV,	)	
	)	RULING OF THE COURT
Defendant.	)	
	)	

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE RICHARD A. JONES
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:
SETH WILKINSON
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:
JOHN HENRY BROWNE
EMMA SCANLAN
Law Offices of John Henry Browne, P.S.
108 S Washington Street
Seattle, WA 98104

Reported by:
NANCY L. BAUER, CCR, RPR
Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
(206) 370-8506
nancy_bauer@wawd.uscourts.gov

June 23, 2016 2:00 p.m.

PROCEEDINGS

THE CLERK: We are here in the matter of United States v. Roman Seleznev, Cause No. CR11-70, assigned to this court.

Counsel, please make your appearances for the record.

MR. WILKINSON: Good afternoon, Your Honor. Seth Wilkinson for the United States.

THE COURT: Good afternoon.

MR. BROWNE: Good afternoon, Your Honor. John Henry Browne and Emma Scanlan on behalf of Mr. Seleznev.

THE COURT: Good afternoon.

THE INTERPRETER: Good afternoon, Your Honor. Linda Noble, state-certified Russian interpreter.

THE INTERPRETER: Good afternoon. Julie Davidov, state-certified Russian interpreter.

THE COURT: Thank you.

My same direction and guidance to the interpreters. If at any point in time this court is going too fast, just raise your hand, or if you need a break to transition between the two of you, again, just raise your hand, let the court know, and I'll be happy to stop. Is that acceptable to both interpreters?

The court summoned the parties today for purposes of the court giving its ruling. The court makes the following

determination:

The defendant seeks to suppress all evidence obtained from the Sony laptop that was seized from the defendant on July 5, 2014. This motion is based upon these grounds:

First, that the affidavit submitted in support of the application to search the laptop relied upon stale information that fails to establish probable cause existed to conduct the search; second, that the 23-day delay in applying for a warrant to search the laptop was an unwarranted delay that prejudiced the defendant by creating an opportunity for the data on the laptop to be altered; and third, that the laptop was so mishandled by the United States Secret Service, that all of the evidence obtained from the laptop should be excluded due to, at minimum, negligence, but more probably misconduct on the part of the government agents in mishandling the laptop.

The first issue is staleness. The standard to be applied in evaluating this motion requires that the court to evaluate the defendant's claims in light of the particular facts of the case and the nature of the criminal activity and property sought.

The primary focus of the court's analysis is predicated upon the content of the search warrant affidavit. Here the defendant concedes -- and I'm referring to page 7 of their motion -- that, in sum, the affidavit may allege sufficient

facts to support a finding of probable cause, but contends that the critical, nonspeculative information was too stale at the time the search warrant was issued.

The court disagrees. The lengthy search warrant affidavit provided a long and detailed chronological history of the alleged credit card trafficking activities of the defendant.

The affidavit also detailed the direct evidentiary connection between the defendant's earlier hacking and credit card trafficking and ongoing hacking and credit card trafficking in the weeks leading up to the defendant's apprehension.

The affidavit also explained that undercover purchases through July of 2014 confirmed defendant was trafficking in stolen credit cards on his new vending site 2pac.cc, providing further direct evidence in support of probable cause.

The affidavit further provided circumstantial evidence that the administrator of the 2pac site stopped posting at or near the time of the defendant's arrest, a fact further confirmed by DOJ Executive Carroll's testimony at the suppression hearing.

Additionally, the agent provided detail related to the defendant's e-currency accounts used to facilitate the defendant's alleged scheme over the course of several years. He also detailed tracing the use of those accounts to a new

credit card vending site that was operating up to the week prior to the defendant's arrest.

This level of detail in the affidavit leading up to the time of the defendant's arrest clearly demonstrates the staleness as a basis for the suppression of the evidence should be denied.

The defendant also seeks to suppress based upon the 23-day delay in obtaining the warrant. The court assesses this motion using a reasonableness standard in light of the totality of the circumstances.

The facts the court has considered in making this determination include, first, the original Assistant United States Attorney had retired, and the case agent preparing the search warrant affidavit was new to the case.

Second, the case investigation had been going on for a protracted period of time, generating a voluminous file to review by the newly-assigned case agent. This file included several years of complex investigative reports, search warrant affidavits, forensic examination reports, and subpoenas.

Three, according to his sworn testimony, Agent Fischlin started working on the affidavit on July 8th, or shortly after the defendant's arrest on July 5. He prepared and submitted the first draft of the search warrant to the Assistant United States Attorney by July 10. The second

draft was prepared while he was in Guam just days later.

Fourth, while preparing the search warrant and exchanging drafts with the Assistant United States Attorney, the case agent was required to travel on July 19 to participate in an identity hearing for the defendant in Guam, which was originally scheduled for July 22 and subsequently postponed to July 31st. This extensive air travel was undertaken with minimal notice, and the final draft of the search warrant was July 22.

Fourth, the preparation of the affidavit by the case agent required digestion of expert testimony about electronic devices and details of a complicated electronic investigation. These details included extensive background testimony on the operation of cyber criminals, credit card trafficking, and review of the complex 2pac domain.

Fifth and last, apparently due to his extended stay in Guam due to a postponement of Mr. Seleznev's hearing, Agent Fischlin sought the assistance of another agent, LaTulip, in Washington, D.C., who had some familiarity with the case, who then travel to Seattle to swear out the affidavit.

The court finds that, in light of all these circumstances, the 23-day delay was reasonable. This was a complicated investigation with extraordinary facts, justifying the delay in obtaining the warrant.

From the testimony of the involved agents, the court finds

there was no unreasonable delay in the efforts by government agents obtaining the warrant.

No case authority posited by the defense comes close to the extraordinary circumstances of what transpired from the date of defendant's arrest to the issuance of a warrant. It appears the agents' efforts were diligent, and they engaged in reasonable efforts to expedite issuance of a warrant without unwarranted delay.

These events and the actions of the agents come nowhere close to the claims of gross incompetence or intentional acts by the agents to warrant suppression.

The court also has taken into consideration the effect of the delay upon the defendant. The court notes the defendant was in custody, and there's no evidence he requested return of the computer. Consequently, any possessory interest he had in the computer was minimal.

For all these reasons, the defendant's request to suppress evidence based upon the 23-day delay is denied.

Last, the defendant seeks suppression of the laptop, contending that the government agents engaged in misconduct by conducting illegal, warrantless searches after July 5, and specifically on July 7, and that the agents mishandled the laptop throughout their time of possession and examination.

Specifically, the defense contends a logon to the laptop occurred two days after the computer was seized in the

Maldives and before a search warrant had been obtained and that this user activity constituted a Fourth Amendment violation warranting suppression.

Before the court are competing experts about what impact, if any, occurred in the computer as a result of how it was handled after it was seized by government agents. The defense experts contend the computer logs clearly demonstrate tampering, access, and alteration of the files by someone other than the defendant.

To the contrary, the government experts contend the Windows operating system and logs overwhelmingly demonstrate the last logon, other than updates, was at a time when the laptop was still in possession of the defendant.

At the outset, the court concludes that the challenges of the reliability of the evidence and the credibility of the witnesses and believability of the expert testimony are factual determinations more appropriately approached as an issue going not to the admissibility but to the weight of the evidence.

It is within the court's province to resolve these competing opinions and determine what weight to accord the government's evidence. Strike that. It is within the jury's province to resolve these competing opinions and determine what wait to accord the government's evidence.

In support of this conclusion, the court directed the

parties to consider *United States v. Golb*, found at 69 F.3d 1417, 1428 specifically, Ninth Circuit opinion 1995. This case involved government and defense competing expert opinions on the experience on the detection of cocaine on dollar bills.

The court also directed the parties to consider also *United States v. Chischilly*, spelled C-h-i-s-c-h-i-l-l-y, found at 30 F.3d 144, Ninth Circuit opinion 1994. This case goes all the way back to the days when admissibility of DNA evidence was challenged when duelling expert opinions were present.

In both circumstances the Ninth Circuit reached the same result as the ruling of this court today. When duelling or competing experts serve as the basis of the challenge, the challenge goes to the weight and not the admissibility, and it becomes a jury determination.

While the court can stop here and rule no further, I will explain the reasoning of the court, view the evidence presented at the suppression hearing, and explain why the court reaches its conclusions.

The defense contends that after seizing the laptop, a user, presumably a law enforcement officer, on July 7th, 2014, logged on to the laptop and logged into the Windows user account for Smaus.

Once logged on, the user had unfettered access to all the

files on the laptop. Specifically, the defense experts contend that a user logon to the Smaus Windows user account on July 7, 2014, as evidenced by a screenshot of a portion of a winlog file. The defense expert also contends the laptop could have connected to an unknown wireless network or wi-fi networks while in connected standby.

The government's expert opined the laptop showed it had not connected to any network subsequent to the 5th of July, and it was impossible to connect remotely to a computer that did not have network access.

The government's expert, Ovie Carroll, his opinion was based upon a series of screenshots from the laptop's forensic image. Carroll referenced a host of registry keys to support his findings and conclusions; one, the network profile key, a registry key that documented every network ever connected to it. According to Carroll, this registry records the first and last time and how one connected to the network. In this case, the last network, according to the noted registry, was the Kanifushi network, which shows it was first connected to the network on June 21 and the last time on July 3rd.

Second, Carroll's opinion also referenced the Windows network profile operational event log. This log keeps track of when a computer connects to and disconnects from the network. According to Carroll, the last recorded entry shows the computer recorded a network connection of July 5 from the

Kanifushi network.

Three, Carroll also referenced the Windows update log, which he characterized as an audit log file, which shows every time Windows tries to connect to the Microsoft server. This log ostensibly tells you its status and the last time the network status was connected. According to Carroll, the log shows the last time the network was connected was July 5, and never regained a network connection.

Fourth, Carroll also relied upon the Windows database that keeps track of the information about the computer for diagnostic purposes. In this case, the diagnostic log is SRUM, which is the System Resource Usage Monitor. This is a log that keeps track of all the applications that are running, and, according to Carroll, the log showed the Kanifushi network was the last network the computer connected to.

Carroll opined that if the computer had connected to the network, there are forensic artifacts, for example, the SRUM database, that would have recorded the event, and other registration keys would have recorded it. His conclusion is that no such evidence or record exists.

Five, Carroll also identified the security event log as the authoritative and most reliable logon and logoff record on the computer system. The log reportedly evidenced that the last user was Smaus, and this was the defendant's

security identifier. Carroll testified that he examined every logon and logoff after June 5, and there were no other user logoffs.

Six, next is the SAM registry file, or software registry file, that deals with the output of the application resource tables in the SRUM database. This operation supposedly keeps track of system diagnostic information and events. The evidence suggested by Carroll is that this keeps track of every application that is running and who is responsible for running that application. His opinion was that the last application user was the Smaus user account, and those were run on July 5.

Seven, the USN journal log, according to Carroll, documents files that are touched so as to affirm they're working and to know what's changing. His opinion was that he reviewed all of the activity after July 5 and found no user activity.

Eight, according to the defense expert, someone logged on to the computer based on the winlogon registry key. According to the defense expert, this is definitive proof that someone logged on to the system post July 5.

To counter this conclusion, Carroll conducted five or six tests where he restarted the image or restarted the computer. The ranges of times varied from one hour, 24 hours, and 48 hours. The defense expert ran no such comparable tests for

similar duration and time; at best, one test for a few minutes. Carroll criticized the defense expert, indicating that in his 20 years of experience he had never heard of any forensic examiner presenting a winlog key as definitive proof of when someone logged on to a computer. Rather, he concluded that the winlog key changes even without logging on to a computer.

Ninth, Carroll also addressed the access times and file modifications referenced by the defense experts after the laptop had been seized by law enforcement.

He explained these as being consistent with McAfee antivirus log files being updated and the Sony laptop having home improvement or normal system maintenance and operations but not user-initiated files.

Tenth and final, Carroll also addressed the splash screen episode noted by one of the agents after seizure of the laptop. He concluded this was part of the mechanics of this type of laptop. When the battery reached two percent, it was trickling down to a low power, and then the laptop went into last possible battery usage or hibernation as a reason for this episode.

These are some of the most significant point/counterpoint issues raised by the parties. The overwhelming weight of the evidence indicates that all of the activity on the laptop after July 5, the date of the defendant's arrest, was the

result of background and operating system activity and maintenance, and not from human interaction.

The overwhelming evidence also indicates the laptop had not connected to any network after July 3, 2014, when it was connected to the wireless network at the defendant's hotel in the Maldives, the Atmosphere Kanifushi, and certainly not after July 5 when the defendant was arrested.

The court also recognizes the challenges the defense makes as to security concerns in violation of Secret Service procedures for logging in and out of the evidence arena when the laptop was being inspected and data recorded.

While the agency may have violated internal procedures for logging in and out, the court does not find any compromise in the security of how the device was handled. The unrebutted evidence indicates the computer was received and placed in a main evidence vault limited to supervisors and administrative officers, and that area was generally restricted to other agents. There were locks, codes, and adequate security about the computer to conclude that it was in a safe and secure overall environment. Any evidence of tampering consequently had to come from the evidence and the experts. The court has found that has not been established, at least to the degree to warrant suppression.

For all these reasons, the court concludes there is no basis to grant the defendant's motions to suppress. At best,

the defendant can present his arguments to the jury, but the evidence and argument presented will not support a motion to suppress.

As I began my analysis, I conclude with the same finding, that the challenge of the defense goes to the weight to be accorded to the evidence, not its admissibility. For all these reasons, the defendant's motions to suppress are all denied.

Counsel, that's the court's finding and determinations. The court will not issue a separate written order. The court is satisfied that is more than ample detail to communicate to the parties the court's ruling.

Anything else to take up, counsel for the government?

MR. WILKINSON: No, Your Honor.

THE COURT: Anything else, counsel for the defense?

MR. BROWNE: No, Your Honor.

THE COURT: All right. We'll be at recess.

(THE PROCEEDINGS CONCLUDED.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 5th day of July 2016.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter